AF
IFW

100.2462
Dempski 1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

| | | |
|---|---|---|
| In re Application of | : | |
| For: | : | Method and System for Collecting Data on the Internet |
| Serial No. | : | 09/497,006 |
| Filed | : | 02/02/2000 |
| Group | : | 2141 |
| Examiner | : | Kang, Paul H. |

Durham, North Carolina
September 10, 2004

MAIL STOP APPEAL BRIEF – PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**Transmittal of Appeal Brief**

Sir:

Transmitted herewith in triplicate is the APPEAL BRIEF in this application with respect to the Notice of Appeal filed on July 19, 2004.

X Enclosed is a check in the amount of $330.00 to cover the Appeal Brief fee. Please credit any overpayment of charge any underpayment to Deposit Account No. 50-1058.

Our telephone number is: (919) 806-1600.

Respectfully,

Peter H. Priest

Peter H. Priest
Attorney for: Dempski

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner of Patents P.O. Box 1450, Alexandria, VA 22313-1450 on the date set forth below.

Signed: Marianna Tortorelli

Name: Marianna Tortorelli

Date: September 10, 2004

100.2462
Dempski 1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

| | | |
|---|---|---|
| In re Application of | : | |
| For: | : | Method and System for Collecting Data on the Internet |
| Serial No. | : | 09/497,006 |
| Filed | : | 02/02/2000 |
| Group | : | 2141 |
| Examiner | : | Kang, Paul H. |

Durham, North Carolina
September 10, 2004

MAIL STOP APPEAL BRIEF – PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the date set forth below:

Signed: Marianna Tortorelli

Name: Marianna Tortorelli

Date: September 10, 2004

APPELLANT'S BRIEF

Sir:

1. The Real Party In Interest

The real party in interest is the assignee, Lucent Technologies, Inc..

2. Related Appeals and Interferences

None.

## 3. Status of the Claims

This is an appeal from the April 19, 2004 final rejection of claims 1, 3, 4 and 6-22, all of the pending claims. Claims 1 and 3 were rejected under 35 U.S.C. § 103(a) as unpatentable over Haitsuka et al. U.S. Patent No. 6,366,298 B1 ("Haitsuka") in view of Robinson U.S. Patent No. 5,918,014 ("Robinson") and further in view of Shear et al. U.S. App. Patent No. US 2003/0041239 A1 ("Shear"). Claims 4, 6 and 7 were rejected under 35 U.S.C. § 103(a) as unpatentable over Haitsuka, Robinson, Shear and further in view of Kunzinger et al. U.S. Patent No. 6,405,222 B1 ("Kunzinger"). Claims 8-13, 15-18, and 20-22 were rejected under 35 U.S.C. § 103(a) as unpatentable over Haitsuka, Robinson, Shear, Kunzinger and further in view of Davis et al. U.S. Patent No. 5,796,952 ("Davis"). Claims 14 and 19 were rejected under 35 U.S.C. § 103(a) as unpatentable over Haitsuka, Robinson, Shear, Kunzinger, Davis and Thomas U.S. Patent No. 6,128,663 ("Thomas").

## 4. Status of Amendments

The claims stand as last amended in a 37 C.F.R. § 1.114 Submission filed with a Request for Continued Examination. The Submission contained an Amendment After Final which was previously submitted and not entered. In the Submission, claim 1 was amended to add the step "acquiring the end user's consent to upload saved information." Claims 10, 16, and 20 were amended to clarify that a processor operated to request a user's consent in order to upload monitored information. Claim 10 was amended by replacing the wording "select whether to upload" with the wording "consent to uploading." Claim 16 was amended by replacing the wording "selectable operation by an end user" with the wording "acquiring consent to upload said monitored information from an end user." Claim 20 was amended by replacing the wording "said monitored information is being received after selectable operation by an end user" with the wording "said monitored information being received after acquiring consent to upload said monitored information from an end user."

During preparation of this appeal, it was discovered that a minor amendments were needed to address a typographical error and a grammatical error. Consequently, an amendment under 37 C.F.R. §1.116 is being filed along with this appeal brief. Step (d) of claim 1 has been amended to replace term "end users'" with the term "end user's". Thus, correcting a misplaced apostrophe. This amendment is consistent with the antecedent term "end user's" found in the preamble of claim 1. Claim 8 has been amended to replace the pronoun "its" with the pronoun "his or her" to properly match the antecedent term "end user."

## 5. Summary of the Invention

The present invention addresses the needs of web content providers to measure the effectiveness of their website in order to compete and to focus their content appropriately for their subscribers or future subscribers while at the same time maintaining the privacy of individuals. As an analogy, Nielson ratings used in the television market enable television networks to measure the popularity of individual shows and in turn the success of the particular network. The Nielson system collects demographic information and viewing habits of television viewers by requesting viewers to voluntarily participate. Such requests are typically made through the U.S. postal service.

The Internet market has made various attempts to address the problem of measuring the effectiveness of a website. A typical unsophisticated approach uses the "hit" metric to measure the number of times a website is viewed by a user. A more sophisticated approach uses typical

Internet marketing systems which track the behavior of users without their consent to achieve an unrelated objective of focusing advertisements to a user based on tracking the user's patterns of usage of the Internet. These marketing systems typically involve extracting demographic and behavior information from the user without the user's knowledge. The lack of agreement by the user raises privacy issues. Additionally, these marketing systems use the extracted information to transmit focused advertisements to the user. Besides the privacy issues raised, the lack of agreement by the user may adversely affect the user's bandwidth because the user has no control of when data is uploaded to these marketing systems and when advertisements are downloaded to the user.

The present invention relates generally to methods and systems for using a computer to gather information regarding an end user's visits to web pages and a duration and date of each visit, and then pairing this data with the user's demographic data at a data processing computer. Such methods and systems may suitably include the steps of monitoring the web pages the end user visits; recording the duration and date of each visit monitored; saving information recorded in the end user's computer; storing the end user's demographic data in the data processing computer; acquiring the end users' consent to upload saved information; and uploading stored information upon selective operation by the end user from the end user's computer to the data processing computer.

In one embodiment, a method for using a computer to gather information of an end user's visits to web pages and a duration of each visit. By way of example, claim 1 of the present invention reads as follows:

> 1. A method for using a computer to gather information of an end user's visits to web pages and a duration of each visit, the method comprising the steps of:
>
> (a) monitoring the web pages the end user visits;

(b) recording the duration and date of each visit monitored in said step (a);
(c) saving information recorded in said step (b) in the end user's computer;
(d) acquiring the end users' consent to upload saved information; and
(e) uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer, the information saved to the end user's computer in said step (c).

In an exemplary embodiment illustrated in Fig. 1, plug-in software 10 is a software module that can be installed into a web browser on a user's personal computer 12. Plug-in software 10 monitors and records uniform resource locators (URLs) as a user accesses web pages. Plug-in software 10 also records the date of each web page visit, the duration of each visit, and some key words typical of the subject matter of each web page visited. See, for example, the present specification at page 3, lines 22-31.

In the user's personal computer 12, two relational databases are used to record a user's data during each Internet session. The first relational database is a user identification database 18 which contains, for example, each user's user identification code (UIC) and logon name. A user's UIC is unique to each user allowing multiple people to have their habits tracked although they operate the same personal computer at different times, as is typical, for a home computer shared by all members of a family, for example. The second relational database is a URL log – UIC database 20 which holds records including URLs indicating web pages a user has visited, the date of each visit, and the duration of each visit, matched with the user's UIC. See, for example, the present specification at page 4, line 32 – page 6, line 1.

At regular time intervals, for example, once a month, a user will be prompted by plug-in software 10 to voluntarily access a web page at a data processing center 22 web site to consent to uploading the contents of the URL log-UIC database 20 to the data processing center. Only after user consent is obtained, data in this database is transmitted utilizing robust encryption methods.

At the data processing center 22, the information received from the URL log –UIC database 20 is correlated with the user's demographic information. The data processing center 22 retrieves the user's full demographic information based on the user's UIC from a global user demographic database 24. The global user demographic database 24 is populated off-line, for example, during a registration process over the telephone or by conventional mail. Thus, the user's personal demographic information is not transmitted over the Internet.

## 6. The Issue For Review

The issues for review are whether claims 1 and 3 were properly rejected under 35 U.S.C. § 103(a) based on Haitsuka, Robinson, and Shear, whether claims 4, 6 and 7 were properly rejected under 35 U.S.C. § 103(a) based on Haitsuka, Robinson, Shear, and Kunzinger, whether claims 8-13, 15-18, and 20-22 were properly rejected under 35 U.S.C. § 103(a) based on Haitsuka, Robinson, Shear, Kunzinger, and Davis, and whether claims 14 and 19 were properly rejected under 35 U.S.C. § 103(a) based on Haitsuka, Robinson, Shear, Kunzinger, Davis, and Thomas. In other words, were the standards set forth in M.P.E.P § 706.02 for 35 U.S.C. §103(a) properly applied in the present case?

## 7. Grouping of Claims

The rejected claims do not stand or fall together. The claims should initially be considered in Groups I-IV based upon the differences between the independent claims: namely, Group I, claims 1, 3, 4, and 6-9; Group II, claims 10-15; Group III, claims 16-19; and Group IV, claims 20-22.

Regarding Group I, claims 1, 3, 4, and 6-9 address "a method for using a computer to gather information of an end user's visits to web pages and a duration of each visit" comprising specific monitoring, recording, saving, acquiring, and uploading steps.

Regarding Group II, claims 10-15 address "a computer connected to the Internet for gathering information as to which web pages an end user visits, the date of each visit, and the duration of each visit, the end user visiting web pages through a web browser." The computer includes "a first user database for storing the monitored information, said processor saving the monitored information to said first user database, said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet, said user interface displaying the periodic requests to the user."

Regarding Group III, claims 16-19 address "a data system accessed through the Internet for processing end users' Internet visits to web pages and the duration of these visits."

Regarding Group IV, claims 20-22 address a method "for using a data processing system for processing end users' Internet visits to web pages and the duration of these visits," including the steps of storing, receiving, matching, organizing, and repeating. 35 U.S.C. § 103(a), which governs obviousness, indicates that "differences between the subject matter sought to be patented and the prior art" are to be assessed based upon "the subject matter as a whole." Under this analysis, the entirety of each claim must be considered.

Additionally, the dependent claims address a number of further combinations and limitations that do not simply rise or fall with the independent claims as addressed in detail in the Argument below.

## 8. Argument

The rejections under Section 103 did not follow MPEP § 706.02 which states at page 700-21:

> in a rejection based on 35 U.S.C. 103, the reference teachings must somehow be modified to meet the claims. The modification must be one which would have been obvious to one of ordinary skill in the art at the time the invention was made.

In contrast with this clear statement, the Official Action looks to a combination of references addressing different problems in a different context. In one case, the Official Action combines no less than six items of prior art to reject claims 14 and 19. For all the rejections, the relied upon art, taken separately or in combination, does not teach the presently claimed invention. Furthermore, it fails to recognize the problems addressed and advantageously solved by the present invention much less suggest the presently claimed solution. Nonetheless, the Official Action suggests the present claims are obvious therefrom. This finding should be reversed.

### A. The Section 103 Rejections

The art rejections are not supported by the relied upon art. All of the rejections are based on Haitsuka, Robinson, and Shear. Several rejections build upon these three base references, progressively adding in the additional references, Kunzinger, Davis, and Thomas. 35 U.S.C. § 103 which governs obviousness indicates that "differences between the subject matter sought to be patented and the prior art" are to be assessed based upon "the subject matter as a whole". Analyzing the entirety of each claim, the rejections under 35 U.S.C. § 103 are not supported by the relied upon art as addressed further below. Only after an analysis of the individual references has been made can it then be considered whether it is fair to combine teachings. However, as addressed further below, fairness requires an analysis of failure of others, the lack of recognition of the problem, and must avoid the improper hindsight reconstruction of the present invention. Such an analysis should consider whether the modifications are actually suggested by the references rather than assuming they are obvious. The 35 U.S.C. § 103 rejections made here pick and choose elements from at least three separate references and, in one rejection six separate references. The references do not provide the required motivation for making the suggested combination. This approach constitutes impermissible hindsight and must be avoided. As required by 35 U.S.C. § 103, claims must be considered as a whole. When so considered, the present claims are not obvious.

Rejection of Claims 1 and 3 Under 35 U.S.C. §103(a)

Claims 1 and 3 were rejected under 35 U.S.C § 103(a) based on Haitsuka, Robinson, and Shear. Haitsuka, Robinson, and Shear are markedly different from the present invention and address problems only peripherally related to the solutions provided by the present invention. Haitsuka is entitled "Monitoring of Individual Internet Usage." Haitsuka addresses methods and apparatus for monitoring on-line activities of an on-line user in order to display advertisements targeted to the user's on-line activities. Haitsuka, col. 3, lines 1-19. The text at col. 4, lines 42-43 of Haitsuka discloses a monitoring server 130 disposed in a network to perform user activity monitoring along with a client monitoring application 110 running on a user's machine. Each time the user performs on-line activity, the client monitoring application communicates with the monitoring server. Haitsuka, col. 5, lines 44-58. This simultaneous communication between the client monitoring application 110 and the monitoring server 130 during the time the user is on-line utilizes available bandwidth which would otherwise be available for the user's on-line activity. While the user is on-line, the monitoring server determines which targeted data needs to be sent to the client monitoring application and then transmits this targeted data to the client monitoring application without any authorization by the user. See, Haitsuka, col. 6, lines 62-66. Most any Internet user can attest to how annoying it s to receive unsolicited and unauthorized targeted data.

In contrast to Haitsuka, the present invention addresses gathering information at the user's computer for subsequent reporting to a data processing computer at a time selected by the user. One advantageous aspect of the present invention is that it avoids the unauthorized use of user bandwidth integral to Haitsuka's approach. As taught by the present invention, the user is prompted at the expiration of a pre-defined time interval to voluntarily upload the recorded information. Such user control allows the user to postpone any user bandwidth impact resulting from uploading the stored information. Claim 1 reads as follows:

> A method for using a computer to gather information of an end user's visits to web pages and a duration of each visit, the method comprising the steps of:
>
> (a) monitoring the web pages the end user visits;
> (b) recording the duration and date of each visit monitored in said step (a);
> (c) saving information recorded in said step (b) in the end user's computer;
> (d) acquiring the end user's consent to upload saved information; and
> (e) uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer, the information saved to the end user's computer in said step (c). (emphasis added)

The final Official Action cites col. 2, lines 51-67, col. 5, lines 23 – col.6, line 3 and col. 6, line 34-45 of Haitsuka as standing for the uploading step. However, Haitsuka at col. 2, lines 51-67 merely describes a need for a targeted advertisement system that can provide information as to the characteristics of those who were exposed to each advertisement. Additionally, Haitsuka states at col. 5, lines 44-50 "[e]ach time an individual uses the local device 100 to connect to the data access network 120, the client monitoring application 110 and the monitoring server establish a session. In this session, the client monitoring application 110 transmits certain information regarding the user of the local device 100 and his use of the local device 100 while connected to the data access network 120." Haitsuka at col. 6, lines 42-45 further states "[e]ach time the local device 100 connects to the monitoring server 130, the client monitoring application 110 preferably sends data indicating the local device's current geographical location to the monitoring server 130." Such text describes Haitsuka's unauthorized usurping of user bandwidth, a problem advantageously addressed by the present invention. Accordingly, Haitsuka very clearly does not teach and does not suggest uploading information upon a "selective operation by the end user" as claimed in presently amended claim 1. Also, Haitsuka does not teach and does not suggest acquiring the end user's consent to upload saved information as in claim 1. See also claim 10 which requires "said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet". (emphasis added) See also, claims 16 and 20 which require "said monitored information is received after acquiring consent to upload said monitored information from an end user".

Robinson fails to cure the deficiencies of Haitsuka as a reference. Robinson addresses a system and apparatus for determining which advertisement to display to a particular on-line user. Robinson, col. 2, lines 9-17. To this end, Robinson's approach involves classifying users having similar interests into a "community" based on the theory that people with similar interests would likely be interested in the same advertisements. Robinson, col. 2, lines 20-27. At col. 2, lines 48-57, Robinson's disclosure suggests means of tracking user's activities such as through the use of "cookies." Notwithstanding Internet browser configuration options which affect the Internet browser's general behavior with respect to cookies, the cookie model of programming involves a Web server fetching the information stored on the user's machine without providing the user the option to not release the cookie information. See the Understand Cookies section and the Usefulness of Cookies section of *Using Cookies* available at http://studio.tellme.com/vxml2/ovw/cookies.html#cookies_101, for example. The remainder of the cited portion of Robinson does not teach and does not suggest acquiring the end user's consent to upload saved information as in claim 1. Also, Robinson does not teach and does not suggest "uploading upon selective operation by the end user from the end user's computer to the data processing computer" as claimed in claim 1. Similarly, see claim 10 which requires "said processor periodically requests the user at the expiration of a predefined time interval to select whether to upload the monitored information to a data processing computer through the Internet." See also, claims 16 and 20 which require "said monitored information is received after acquiring consent to upload said monitored information from an end user."

Shear fails to cure the deficiencies of Haitsuka and Robinson. Shear is entitled "Systems and Methods Using Cryptography to Protect Secure Computing Environments." Shear addresses the problem of providing secure computation and execution spaces in a computing environment. To this end, Shear describes a verifying authority that digitally signs and certifies load modules or executables which are typically received by the computer system. Shear, para. [0033]. During a telephone interview with the Examiner on May 25, 2004, it was pointed out that the software verification and authentication techniques described in Shear are not user consent as claimed in claim 1. In Shear's described techniques, the object of the verification or authentication is a software load module or other suitable executable. Shear merely describes software verification techniques to ensure that downloaded software cannot damage a computer system.

In stark contrast to the relied upon art, the present invention acquires user consent to upload saved information stored on the user's computer such as indications of web pages visited and the amount of time spent at each visited web page.

Haitsuka, Robinson, and Shear, taken seperately or taken in combination, do not teach and do not suggest acquiring the end user's consent to upload saved information from the end user's computer in the manner claimed. Further, Haitsuka, Robinson, and Shear, taken seperately or taken in combination, do not teach and do not suggest uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer as claimed.

By contrast, to the extent Haitsuka, Robinson, and Shear deal with monitoring user activity and uploading the monitored activity, they do so without acquiring the consent of the end user. Further, Shear deals with securing computer systems by performing various validation techniques on software modules and is not relevant to the art of monitoring user activity over the Internet.

Cleary, the relied upon art does not teach and does not render obvious the presently claimed techniques, all of which address aspects of obtaining end user consent before uploading information from the user's computer. See claim 1, for example, which recites "(d) acquiring the end user's consent to upload saved information; and (e) uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer, the information saved to the end user's computer in said step (c)." See also claim 10, for example, which recites "said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet, said user interface displaying the periodic requests to the user." See also claim 16 which recites "said monitored information being received after acquiring consent to upload said monitored information from an end user." See also claim 20 which recites "receiving uploaded monitored information …said monitored information being received after acquiring consent to upload said monitored information from an end user." Thus, independent claims 1, 10, 16 and 20 should be allowed over the relied upon art.

The Response to Arguments section of the final Official Action suggests that Shear at paras. 0037-0040 provides for manual authorization of executables wherein a user provides permission to access data. First, the Applicant respectfully disagrees that the cited portion of text supports the suggestion. Second, even if the cited portion of text did support the suggestion, the Applicant believes such suggestion is irrelevant since the present invention addresses acquiring the user's consent to upload saved information to a data processor. The end user is not consenting to accessing the data as the final Official Action suggests. Put otherwise, consent to download is different than consent to upload.

Claim 3 depends directly from claim 1, incorporating all of the limitations thereof and adding further limitations thereto. Claim 3 adds additional classifying and recording steps. Specifically, claim 3 recites "classifying a subject matter of each web page visited; and recording the subject matter in step (b)." These further features provide an independent basis for allowance over the relied upon art.

Rejection of Claims 4, 6, and 7 Under 35 U.S.C. §103(a)

Claims 4, 6, and 7 were rejected under 35 U.S.C § 103(a) based on Haitsuka, Robinson, Shear, and Kunzinger. Kunzinger fails to cure the deficiencies of Haitsuka, Robinson, and Shear described above. Kunzinger describes a system which concurrently displays a set of web pages in a distributed database with a minimum of user interactions to improve the use of bookmarks in web browsers. Kunzinger, Abstract. To this end, Kunzinger's web server compresses and decompresses related web pages for concurrent display. Kunzinger, col. 9, lines 22-24.

Unlike Kunzinger, the present invention compresses and encrypts information monitored and saved at an end user's system. Claim 4 which depends on claim 1 recites "wherein the information saved in step (c) is compressed and encrypted." Step (c) in claim 1 recites "saving information recorded in said step (b) in the end user's computer." Kunzinger does not suggest and does not teach compression and encryption in the manner claimed in claim 4.

Moreover, unlike the features of claim 6, Haitsuka's approach does not teach and does not suggest ensuring privacy by uploading saved information containing a user identification code that <u>relates</u> to the end user's demographic information stored at a data processing system. (emphasis added) This feature in the present invention provides further insurance of end user privacy, for example, because the end user code itself contains no information related to the end user which could be tapped by attaching a network analyzer monitoring network transmissions. Claim 6 recites "wherein the information saved in said step (c) is stored under an end user's user identification code." Claim 11 requires that the "monitored information is paired with end user's user identification code."

In the Response to Arguments section, the final Official Action suggests that Haitsuka at col. 5, line 23 – col.6, line 53 clearly teaches a user identification that relates to the end user's demographic information. It should be noted that the Applicant asserts that Haitsuka does not teach and does not suggest ensuring privacy by <u>uploading</u> saved information containing a user identification code that relates to the end user's demographic information stored at a data processing system. (emphasis added) The final Official Action inappropriately seeks to focus on only a portion of this limitation as claimed. Haitsuka at col. 5, line 59 – col. 6, line 3 discloses uploading personal profile information from the client monitoring application. The personal profile information includes age, sex, home address, and the like. By uploading this information, Haitsuka clearly teaches away from the present invention which uploads a user identification code which is correlated with personal information at a data processing system.

Rejection of Claims 8-13, 15-18, and 20-22 Under 35 U.S.C. §103(a)

Claims 8-13, 15-18, and 20-22 were rejected under 35 U.S.C § 103(a) based on Haitsuka, Robinson, Shear, Kunzinger, and Davis. Davis fails to cure the deficiencies of Haitsuka, Robinson, Shear, and Kunzinger described above. Davis describes a method for monitoring a client interaction with a resource downloaded from a server in a computer network. Davis, Abstract. To this end, Davis's approach includes embedding a tracking program with the downloaded resource. The tracking program starts a timer while the user uses the downloaded resource. When the downloaded resource is a web page, once the user leaves the web page the tracking program sends the monitored time to another computer on the Internet for storage and analysis. See Davis, col. 9, lines 3-15. Because the tracking software is embedded in the downloaded resource, a user of Davis's system is unaware of the information gathered and the event of the timer being expired and is not provided control over of the timing of when uploading of information occurs.

In stark contrast to Davis, the present invention acquires the user's consent for uploading monitored information. For example, the user may log on to the system before each web session by identifying himself or herself as shown in Fig. 2 by providing the user's identification code or user name. See page 11, lines 7-11. Further, referring to page 7, lines 6-9, the user, by other means than the network, registers personal demographic information for entry into the global user demographic database to ensure privacy and consent, for example. The present invention's data processing center 22 "never prompts an end user to upload any information and never receives any data unless the user voluntarily uploads the data." Specification, page 11, lines 31-33. See independent claim 10 which requires "said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet", independent claim 16 which requires "said monitored information being received after acquiring consent to upload said monitored information from an end user", and independent claim 20 which requires the step of "receiving uploaded monitored information from an end user's computer wherein said monitored information including the URLs visited by end users and the duration of time spent visiting these URLs, said monitored information being received after acquiring consent to upload said monitored information from an end user."

The April 19, 2004 final rejection relies on Davis as purportedly making obvious the limitations specified in claims 8 and 9. Claim 8 refines the step in claim 1 of uploading saved information upon selective operation by the end user. Specifically, claim 8 addresses "requesting the end user to upload the saved information upon expiration of a user defined time interval ... prompting the end user for its user identification code or user name; inputting the end user information on the end user's computer; and uploading the entered user identification code and the saved information to a data processing computer without receiving any information from the data processing computer to be displayed to the end user." Unlike the user defined time interval of claim 8, Davis's tracking program automatically starts a timer upon download of the resource. Furthermore, such a technique of uploading the entered user identification code in claim 8 advantageously allows correlation of user demographics and personal information with saved information to take place on the data processing computer without having to send personal information and demographics over the Internet. Thus, the technique, as claimed in claim 8, saves network bandwidth and secures personal information. Claim 9 is dependent on claim 8 and adds the additional step of "rewarding the end user for choosing to upload the saved information." See also claim 11 which makes clear that monitored information is paired with an end user's user identification.

The final Official Action further relies on Davis as purportedly suggesting a user identification code as claimed in claim 8. Applicant respectfully disagrees. Davis's system captures existing identifying indicia from the client such as any network or client IDs resident in a hypertext transfer protocol (HTTP) request header sent by the client. Davis, col. 5, lines 40-44. Davis's ID is then used in a totally different manner than the manner claimed. IDs are ubiquitous, but claims 8 and 9 do not simply claim an ID. The rejection does not address the claim language in it entirety.

Davis, separately or in combination with the other references, does not teach and does not suggest acquiring the consent to upload monitored information from an end user as claimed. Davis simply embeds a tracking program with the downloaded resource to be tracked with an existing ID. The present invention takes an entirely different approach by tracking users' habits on a voluntary basis to accumulate ratings for visited web sites, a problem which is not addressed in Davis which appears to track automatically whether a user consents or not. In the present approach, the accumulated ratings include associated personal demographics. These accumulated ratings may be subsequently sold to the URLs visited by the voluntary users.

Dependent claims 12 and 13 refine how the processor of claim 10 monitors URLs visited by the end user and the duration of time spent visiting these URLs. Specifically, claim 12 "passively monitors a TCP/IP stack protocol to retrieve the monitored information." In claim 13, the processor "monitors the web browser cache to retrieve the monitored information." Although Davis utilizes the TCP/IP protocol to extract a client ID as described above, Davis does not teach and does not suggest the techniques of monitoring a TCP/IP stack or a web browser cache to retrieve the URLs visited by an end user and the duration of the time spent visiting these URLs as claimed in claims 12 and 13.

Other than broadly rejecting claims 10, 15-18, and 20-22 en masse based on "the same rationale" as claims 1, 3-4, and 6-9, the final Official Action does not address the claim limitations of these claims. Claims 15, 18, and 21 cover certain aspects of the present invention not disclosed in the relied upon art. For example, claim 15 requires "a second database for storing user identification information including a user identification code, said user identification code is used as a key to relate corresponding monitored information in the first user database with the user identification information." Haitsuka, Robinson, Shear, Kunzinger, and Davis, taken separately or in combination, do not teach and do not suggest a second database on computer connected to the Internet which specifically stores a user identification code in the manner claimed. Claim 18 requires "the demographic information and the monitored information include an end user identification code for matching monitored information with demographic information." Claim 21 requires "comparing an end user identification code stored with the end user information with an end user identification code carried in the uploaded monitored information." Haitsuka, Robinson, Shear, Kunzinger, and Davis, taken separately or in combination, do not teach and do not suggest the features specified in claims 10, 15-18, and 20-22.

Rejection of Claims 14 and 19 Under 35 U.S.C. §103(a)

Claims 14 and 19 were rejected under 35 U.S.C. § 103(a) based on Haitsuka, Robinson, Shear, Kunzinger, Davis, and Thomas. Thomas describes a system for customizing web pages based on demographic information stored on a client's computer. The final Official Action apparently relies upon Thomas for its disclosure related to encrypting and compressing demographic information.

Unlike Thomas, the present invention not only does not compress demographic information it does not upload demographic information over the network. Demographic data is supplied off-line to the data processing center for input to the global user demographic database, for example, during a registration process over the telephone or by conventional mail. Specification, page 7, lines 6-9. The final Official Action apparently misreads the language of the claim. The present invention uploads a user identification code which is mapped to demographic information at a global user demographic database. There are no pending claims and the specification does not support compressing demographic information. Thus, Thomas is irrelevant to claims 9 and 14.

In the Response to Arguments section, the final Official Action rejects the argument above because "the features upon which applicant relies (i.e., off-line supply of demographic information) are not recited in the rejected claim(s)." In other words, it appears from this exchange with the Office that the Applicant is required to claim the negative limitation of not uploading demographic information. It would be burdensome, if not impossible, for an

Applicant to claim every limitation that a present invention is not. Furthermore, the feature of not uploading demographic information is implicit in the claims, however, because claims 10 and 16, upon which claims 14 and 19 depend, recite uploading monitored information which is defined to include "URLs visited by the end user and the duration of time spent visiting these URLs." The definition of the term "monitored information" in the claims in addition to the specification's specific disclosure that demographic information is supplied off-line, the term "monitored information" should not be interpreted to include demographic information. Thus, encrypting and then uploading demographic information as taught in Thomas is not relevant.

The final Official Action attempts to vitiate Applicant's discussion of the references by insisting that Applicant must discuss them "in combination". Granted that the rejection is based on various combinations, the references can only be discussed sequentially in the context of their own words. Applicant is not required to accept the argument that the combination is justified. Applicant likewise is not required, assuming for the sake of discussion that the combination is justified, to accept the further argument that the subject claims are rendered obvious by the combination. Here, the proposed combination is not justified, because a verifying authority for verifying load modules and executables is not acquiring user consent, and because a verifying authority as taught by Shear is not a system which tracks user's habits on the Internet. Assuming without agreeing that the combination is justified, modifying Haitsuka and Robinson with the teachings of Shear still does not produce the method of claims 1 and 20, the apparatus of claim 10, or the system of claim 16, because neither reference discloses and neither reference suggests a method, apparatus, or system for gathering information of an end user's visits to web pages and a duration of each visit by acquiring the end user's consent before uploading the saved information.

Dependent Claims

Claims 3, 4, and 6-9 depend directly or indirectly from claim 1, incorporating all of the limitations thereof and adding further limitations thereto. Claims 11-15 depend directly from claim 10, incorporating all of the limitations thereof and adding further limitations thereto. Claims 17-19 depend directly from claim 16, incorporating all of the limitations thereof and adding further limitations thereto. Claims 21 and 22 depend directly from claim 20, incorporating all of the limitations thereof and adding further limitations thereto. These dependent claims are allowable based upon their dependence on allowable independent claims and the arguments presented above addressing the features of these dependent claims not found in the applied references.

To sum up, Haitsuka, Robinson, and Shear do not show and do not suggest methods, an apparatus, and a system for gathering information of an end user's visits to web pages and a durations of each visit which includes acquiring the end user's consent to upload saved information and uploading saved information upon selective operation by the end user. Nothing in the relied upon references indicates a recognition of the problems addressed by the present invention. Further, nothing in the relied upon references indicates a system which would solve the problems addressed by the present invention. The claims of the present invention are not taught, are not inherent, and are not obvious in light of the art relied upon.

B. The Examiner's Findings of Obviousness are Also Contrary to Law of the Federal Circuit

As shown above, the invention claimed is not suggested by the relied upon prior art. The references cited by the Examiner, if anything, teach away from the present invention. It is only in hindsight, after seeing the claimed invention, that the Examiner could combine the references as the Examiner has done. This approach is improper under the law of the Federal Circuit, which has stated that "[w]hen prior art references require selective combination by the Court to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight gleaned from the invention itself." Uniroyal, Inc. v. Rudkin-Wiley Corp., 5 U.S.P.Q. 2d 1434, 1438 (Fed. Cir. 1988), cert. den., 102 L.Ed. 2d 51 (1988); quoting Interconnect Planning Corp. v. Feil, 227 U.S.P.Q. 543, 535 (Fed. Cir. 1985). Furthermore, "[i]t is impermissible to use the claims as a frame and the prior art references as a mosaic to piece together a facsimile of the claimed invention." Uniroyal Inc. v. Rudkin-Wiley Corp., 5 U.S.P.Q. 303, 312 (Fed. Cir. 1983), cert. den., 469 U.S. 851 (1984). Similarly, "[t]he mere fact that the prior art could be so modified would not have made the modification obvious unless the prior art suggested the desirability of the modification." In re Laskowski, 10 U.S.P.Q. 2d 1397, 1398 (Fed. Cir. 1989), quoting In re Gorgon, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984). No such suggestion is found here.

In addition, the Examiner does not appear to have considered "where the references diverge and teach away from the claimed invention", Akzo N.V. v. International Trade Commission, 1 U.S.P.Q. 2d 1241, 1246 (Fed. Cir. 1986), cert. den., 482 U.S. 909 (1987); and W.L. Gore Associates, Inc., 220 U.S.P.Q. at 311; nor has the Examiner read the claims as a whole, as required by statute. 35 U.S.C. §103. See also, Smithkline Diagnostics Inc. v. Helena Laboratories Corp., 8 U.S.P.Q. 2d 1468, 1475 (Fed. Cir. 1988); and Interconnect Planning Corp., 227 U.S.P.Q. at 551.

In In re Laskowski, 10 U.S.P.Q. 2d 1397, the Federal Circuit reversed an obviousness rejection of the claims in an application for a bandsaw. The claimed bandsaw used a pulley type wheel loosely fitted with a tire. The primary reference showed a similar bandsaw where the band was tightly fitted. The Federal Circuit stated that the prior art did not provide a suggestion, reason or motivation to make the modification of the reference proposed by the Commissioner. Id. at 1398. The Court added that "there must be some logical reason apparent from the positive, concrete evidence of record which justifies a combination of primary and secondary references." Id. quoting In re Regal, 188 U.S.P.Q. 136, 139 (C.C.P.A. 1975), citing In re Stemniski, 170 U.S.P.Q. 343 (C.C.P.A. 1971).

In Uniroyal Inc. v. Rudkin-Wiley Corp., 5 U.S.P.Q. 2d 1434 (Fed. Cir. 1988), cert. den., 102 L.Ed. 2d 51 (1988), the Federal Circuit reversed the District Court's finding that the claims for a patent for an air flow deflecting shield were obvious. Without any suggestion in the art, the District Court improperly chose features from several prior art references to recreate the claimed invention.

The Examiner's rejection suggests that the Examiner did not consider and appreciate the claims as a whole. The claims disclose a unique combination with many features and advantages not shown in the art. It appears that the Examiner has oversimplified the claims and then searched the prior art for the constituent parts. Even with the claims as a guide, however, the Examiner did not recreate the claimed invention.

## 9. Conclusion

The rejection of claims 1, 3, 4 and 6-22 should be reversed and the application promptly allowed.

Respectfully submitted,

Peter H. Priest
Reg. No. 30,210
Priest & Goldstein, PLLC
5015 Southpark Drive, Suite 230
Durham, NC 27713
(919) 806-1600

## APPENDIX
(Claims Under Appeal)

1. A method for using a computer to gather information of an end user's visits to web pages and a duration of each visit, the method comprising the steps of:

(a) monitoring the web pages the end user visits;

(b) recording the duration and date of each visit monitored in said step (a);

(c) saving information recorded in said step (b) in the end user's computer;

(d) acquiring the end user's consent to upload saved information; and

(e) uploading saved information upon selective operation by the end user from the end user's computer to a data processing computer, the information saved to the end user's computer in said step (c).

2. (canceled)

3. The method of claim 1, further comprising the steps of:

classifying a subject matter of each web page visited; and

recording the subject matter in step (b).

4. The method of claim 1, wherein the information saved in step (c) is compressed and encrypted.

5. (canceled)

6. The method of claim 1, wherein the information saved in said step (c) is stored under an end user's user identification code.

7. The method of claim 6, wherein the user identification code is an alpha-numeric character.

8. The method of claim 1, wherein the step of uploading saved information upon selective operation by the end user further comprises:

requesting the end user to upload the saved information upon expiration of a user defined time interval, the saved information further including URLs the user has previously visited and the duration of time the user has spent visiting these URLs;

selecting to upload the saved information;

prompting the end user for its user identification code or user name;

inputting the end user information on the end user's computer; and

uploading the user identification code and the saved information to a data processing computer without receiving any information from the data processing computer to be displayed to the end user.

9. The method of claim 8 further comprising the step:

rewarding the end user for choosing to upload the saved information.

10. A computer connected to the Internet for gathering information as to which web pages an end user visits, the date of each visit, and the duration of each visit, the end user visiting web pages through a web browser, the system comprising:

a user interface;

a processor for running program code to monitor information from the web pages visited by the web browser, the monitored information including URLs visited by the end user and the duration of time spent visiting these URLs; and

a first user database for storing the monitored information, said processor saving the monitored information to said first user database, said processor operating to periodically request the user at the expiration of a predefined time interval to consent to uploading the monitored information to a data processing computer through the Internet, said user interface displaying the periodic requests to the user.

11. The computer of claim 10 wherein monitored information is paired with an end user's user identification code.

12. The computer of claim 10 wherein the processor passively monitors a TCP/IP stack protocol to retrieve the monitored information.

13. The computer of claim 10 wherein the processor monitors the web browser cache to retrieve the monitored information.

14. The computer of claim 10 wherein the monitored information is compressed and encrypted before being uploaded.

15. The computer of claim 10 further comprising:

a second database for storing user identification information including a user identification code, said user identification code being used as a key to relate corresponding monitored information in the first user database with the user identification information.

16. A data system accessed through the Internet for processing end users' Internet visits to web pages and the duration of these visits, the system comprising:

a first database storing user demographic information, said first database populated with user demographic information off-line and with end users' consent;

a processor for receiving uploaded monitored information from an end user's computer, said monitored information including the URLs visited by end users and the duration of time spent visiting these URLs, said monitored information being received after acquiring consent to upload said monitored information from an end user, said processor organizing the received monitored information according to user demographic information stored in said first database; and

a second database for storing the organized information.

17. The data system of claim 16 wherein the processor is operative to receive monitored information without transmitting any information which would be displayed to an end user.

18. The data system of claim 16 wherein the demographic information and the monitored information include an end user identification code for matching monitored information with demographic information.

19. The data system of claim 16 wherein the demographic information comprises the end user's age, sex, ethnicity, nationality, physical disability, and address.

20. A method for using a data processing system for processing end users' Internet visits to web pages and the duration of these visits, the method comprising the steps of:

(a) storing end users' demographic data in a first database of the data processing computer;

(b) receiving uploaded monitored information from an end user's computer wherein said monitored information including the URLs visited by end users and the duration of time spent visiting these URLs, said monitored information being received after acquiring consent to upload said monitored information from an end user;

(c) matching the monitored information with the stored end user information; and

(d) organizing the received monitored information according to the stored end user demographic data.

(e) repeating steps (b) to (d) for more than one end user.

21. The method of claim 20 wherein in said matching step comprises the step of:

comparing an end user identification code stored with the end user information with an end user identification code carried in the uploaded monitored information.

22. The method of claim 20 wherein end users' demographic data comprises an end user's age, sex, ethnicity, nationality, physical disability, and address.